

# OAuth 認証の設定 管理者編

## 目次

|    |                                       |    |
|----|---------------------------------------|----|
| 1. | 概要 .....                              | 2  |
| 2. | Blue Moon の登録について .....               | 3  |
| 3. | Google Workspace .....                | 4  |
|    | 登録手順.....                             | 4  |
|    | Gmail API の有効化 .....                  | 4  |
|    | OAuth 認証画面 .....                      | 6  |
|    | 認証情報 .....                            | 14 |
| 4. | Microsoft 365 (Exchange Online) ..... | 17 |
|    | 登録手順.....                             | 18 |
|    | アプリの登録.....                           | 18 |
|    | 認証 .....                              | 21 |
|    | API のアクセス許可 .....                     | 22 |
|    | ブランドの設定 .....                         | 26 |
|    | ユーザーやグループにアプリを割り当てる .....             | 27 |
|    | アクセス許可（管理者の同意）の付与 .....               | 32 |
|    | 割り当ての確認 .....                         | 33 |
|    | アクセス許可（管理者の同意）の取り消し .....             | 34 |
|    | SMTP AUTH の有効化 .....                  | 35 |
|    | 注意点 .....                             | 38 |
| 5. | 資格情報ファイルの作成 .....                     | 39 |
|    | 資格情報ファイル作成画面の表示.....                  | 39 |
|    | 機能の説明 .....                           | 40 |
|    | 作成手順.....                             | 42 |
| 6. | 注意点 .....                             | 44 |
|    | 自動配信時 .....                           | 44 |

## 1. 概要

この文書は、Blue Moon を自社内の OAuth 認証登録アプリ（内部アプリ）として管理運用するための方法について記述しています。

OAuth 認証に対応したアプリを使用する一般的な方法として、次の 2 つがあります。

### ➤ 外部アプリ：

開発元がクラウドサービスのプロバイダに申請し、Public に外部公開しているクライアント ID を利用しサインインを行う。一般的なメールクライアントアプリ（Outlook や Thunderbird）等がこの方法です。

### ➤ 内部アプリ：

自社内で契約しているクラウドサービス上で、使用するアプリの登録管理を行う。登録時に発行されるクライアント ID を利用しサインインが可能になる。Salesforce 等がこの機能を搭載している。

Blue Moon は、内部アプリに対応しています。特に企業や組織の場合は次の理由から内部アプリとして管理運用することを推奨しています。

- アプリを経由してリソースにアクセスできるユーザーや権限を自社内のポリシーに合わせて制限できる。
- サインインを行ったユーザーを監査ログで確認し不正なアクセス等を調査できる。

また、1日のユーザー承認数（トークン付与数）は、サービスを提供するプロバイダから制限を課されています。Public な外部アプリとして公開した場合は、アクセスするユーザー数も多くなり、不正なアクセスが発生する確率も高くなります。不正なアクセス等が発生した場合は、この制限数が一時的に縮小される可能性も考慮する必要があります。（どの程度縮小されるかについては公表されていない）

大量のメールを配信する場合は、配信に長時間を要し、再接続等を繰り返す必要があります。そのため、安定かつ安全に管理運用を行うには、内部アプリとして登録するほうが効率的となります。

## 2. Blue Moon の登録について

Blue Moon を自社内のアプリとして登録管理するためには、ユーザーが契約しているクラウドサービスの管理ツールを使用する必要があります。現バージョンで対応しているクラウドサービスは、次のようになります。

- [Google Workspace](#)
- [Microsoft 365 \(Exchange Online\)](#)

登録管理を行う方法は、プロバイダの管理ツール毎に異なります。そのため次の章では、上記クラウドサービス毎に手順を説明します。

上記サービスを契約している企業であれば、既に管理ツールの初歩的な操作知識も有していると思われます。そのため、基本的な知識を持つシステム管理者等を前提として説明します。

また、特に難しい操作は無いため、上記サービスを契約している個人ユーザーでも十分に管理運用可能です。

### 3. Google Workspace

アプリの登録を行うには、Google Workspace と紐づいたアカウントで管理できる GCP（Google Cloud Platform）を使用します。

なお、Google Workspace を契約していないユーザーで「gmail.com」のアカウントで OAuth 認証を行う場合も、GCP のアカウントを作成する必要があります。

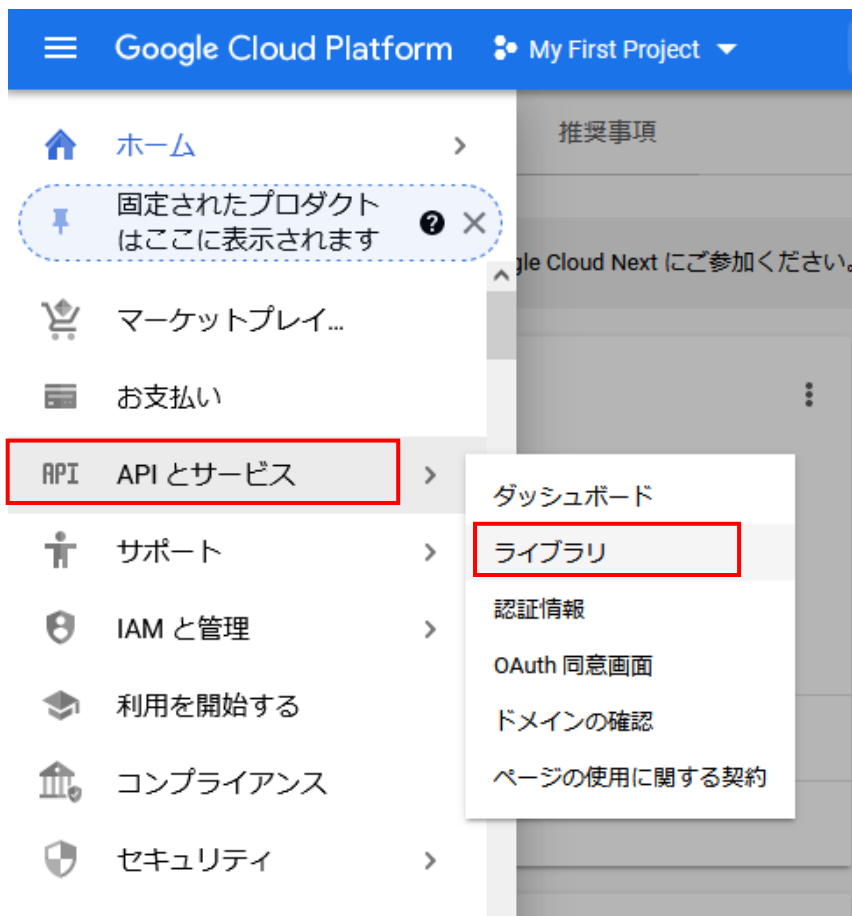
#### 登録手順

GCP 上には、アプリを登録するプロジェクトが既に存在していることを前提に説明します。存在していない場合は作成して下さい。

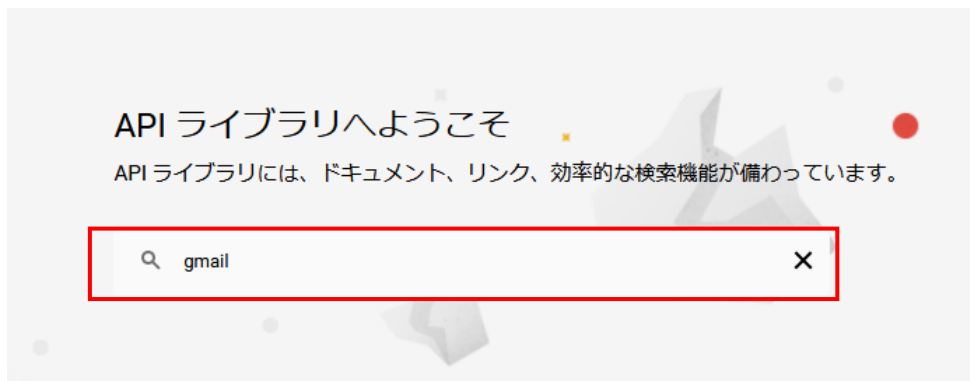
#### Gmail API の有効化

Gmail の API を有効化し、Blue Moon から使用できるようにします。

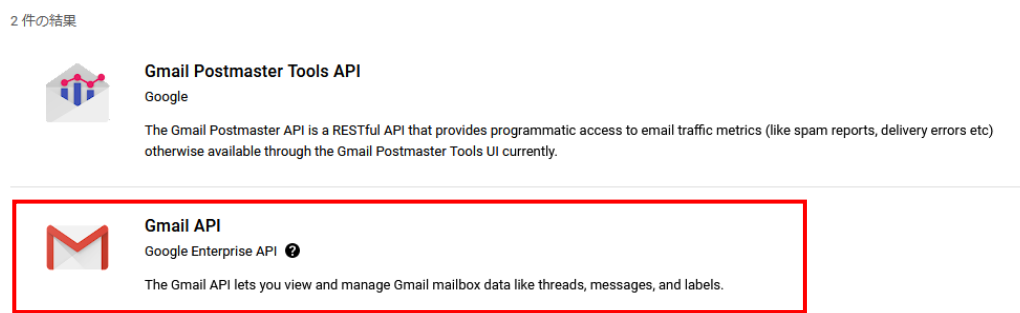
1. メニューの「API とサービス」から「ライブラリ」を選択する。



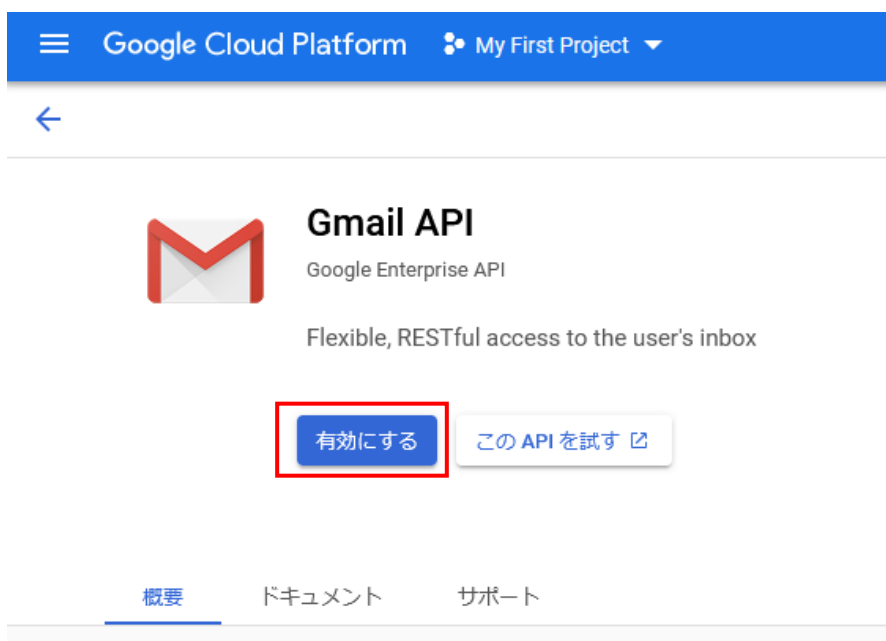
2. 入力ボックスに「gmail」と入力し検索を実行する。



3. 検索結果から「Gmail API」を選択する。

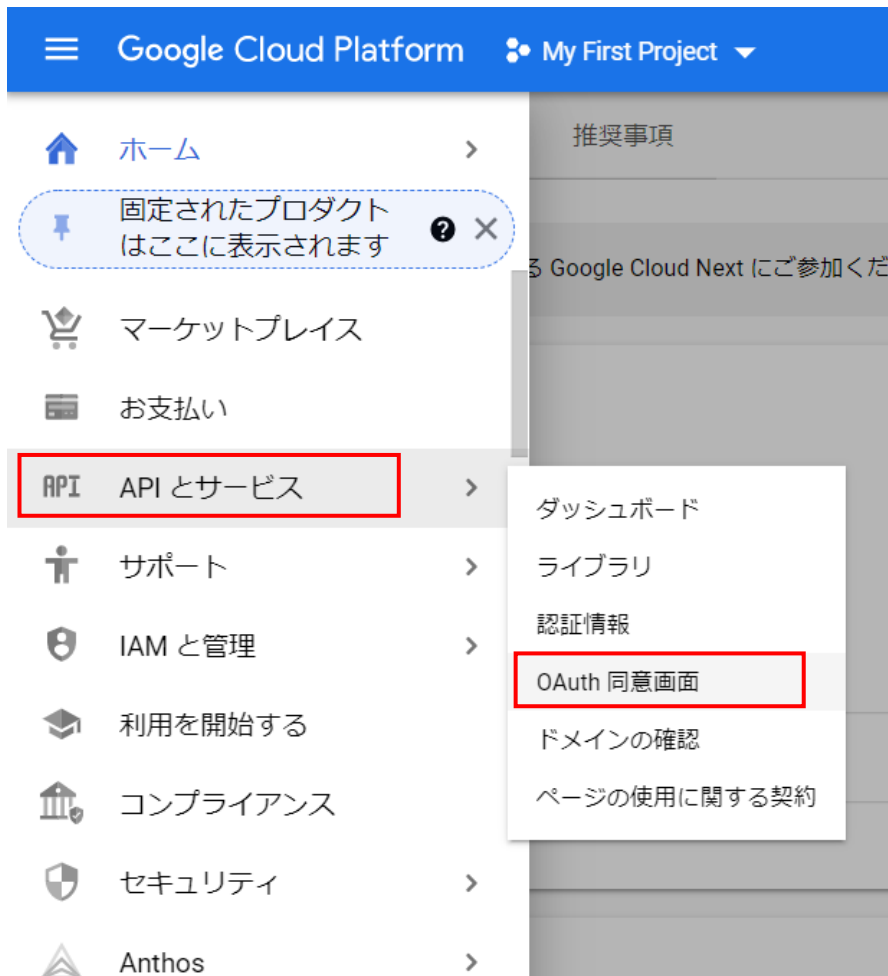


4. 「有効にする」を実行する。



## OAuth 認証画面

1. メニューの「API とサービス」から「OAuth 同意画面」を選択する。



2. OAuth 同意画面の User Type で「内部」を選択し「作成」を実行する。

Google Cloud Platform My First Project

API とサービス

OAuth 同意画面

アプリをどのように構成および登録するか（ターゲット ユーザーを含む）を選択します。プロジェクトに関連付けることができるアプリは 1 つだけです。

User Type

☒ 内部 ?

組織内のユーザーのみが使用できます。確認を受けるためにアプリを送信する必要はありません。 [ユーザーの種類の詳細](#)

☐ 外部 ?

Google アカウントを持つすべてのテストユーザーが使用できます。アプリはテストモードで起動し、アプリを使用できるのは、テストユーザーのリストに追加されたユーザーに限られます。アプリを本番環境に移す準備ができたなら、アプリの確認が必要となる場合があります。 [ユーザーの種類の詳細](#)

作成

Google の OAuth に関する [ご意見やご要望をお聞かせください](#)。

Google Workspace を契約していない個人ユーザー (gami.com アカウント) の場合は、外部のみ選択可能です。外部を選択し、リソースへアクセス可能にするテストユーザーを追加することで OAuth 認証が可能になります。

3. アプリ登録の編集ページで次の様に各項目を入力し、完了後「保存して次へ」を実行する。

#### アプリ情報

| 項目名         | 入力値                    |
|-------------|------------------------|
| アプリ名        | Blue Moon              |
| ユーザーサポートメール | 任意のサポート用メールアドレス        |
| アプリのロゴ      | BlueMoonLogo120.png ※1 |

※1)アプリロゴのダウンロード URL

[https://symmetry-soft.com/software/blue\\_moon/download/logos/logos.htm](https://symmetry-soft.com/software/blue_moon/download/logos/logos.htm)

#### アプリのドメイン

| 項目名                   | 入力値   |
|-----------------------|---|
| アプリケーションのホームページ       | <a href="https://symmetry-soft.com/index.htm">https://symmetry-soft.com/index.htm</a>   |
| アプリケーションプライバシーポリシーリンク | <a href="https://symmetry-soft.com/html/symmetry_soft.htm#privacy">https://symmetry-soft.com/html/symmetry_soft.htm#privacy</a>                                       |
| アプリケーション利用規約リンク       | <a href="https://symmetry-soft.com/software/blue_moon/html/prod_bluemoon.htm#licence">https://symmetry-soft.com/software/blue_moon/html/prod_bluemoon.htm#licence</a> |

#### 承認済みドメイン

アクセスを許可する任意のドメインを追加する。上記アプリのドメインで symmetry-soft.com の URL を使用する場合は、「symmetry-soft.com」の追加が必要です。  
自社内の URL を設定する場合は、その URL を追加して下さい。

#### デベロッパーの連絡先情報

アプリを登録するプロジェクト管理者のメールアドレスを入力する。開発元となる Symmetry Soft のメールアドレスではなく、自社内の管理者の連絡先を入力して下さい。



API API とサービス

- ダッシュボード
- ライブラリ
- 認証情報
- OAuth 同意画面
- ドメインの確認
- ページの使用に関する契約

アプリ登録の編集

1 OAuth 同意画面 — 2 スcope — 3 概要

アプリ情報

この情報は同意画面に表示されるため、デベロッパーのユーザー情報とデベロッパーへの問い合わせ方法をエンドユーザーが把握できます。

アプリ名 \*  
Blue Moon

同意を求めるアプリの名前

ユーザー サポートメール \*  
smsmaster01@symmetry-soft.work

ユーザーが同意に関して問い合わせるために使用

アプリのロゴ  
BlueMoonLogo.png X 参照

ユーザーがアプリを認識できるように、同意画面に 1 MB 以下の画像をアップロードします。使用できる画像形式は、JPG、PNG、BMP です。最適な結果を得るには、ロゴを 120 x 120 ピクセルの正方形にすることをおすすめします。



アプリのドメイン

デベロッパーとユーザーを保護するために、Google では、OAuth を使用するアプリのみに認可ドメインの使用を許可しています。同意画面では、次の情報がユーザーに表示されます。

アプリケーションのホームページ  
https://symmetry-soft.com/index.htm

ホームページへのリンクをユーザーに提供します

[アプリケーション プライバシー ポリシー] リンク  
https://symmetry-soft.com/html/symmetry\_soft.htm#privacy

一般公開のプライバシー ポリシーへのリンクをユーザーに提供します

[アプリケーション利用規約] リンク  
https://symmetry-soft.com/software/blue\_moon/html/prod\_bluemoon.htm#licence

一般公開の利用規約へのリンクをユーザーに提供します

<1

承認済みドメイン 2

同意画面または OAuth クライアントの構成でドメインが使用されている場合は、ここで事前登録する必要があります。アプリの検証が必要な場合は、Google Search Console にアクセスして、ドメインが承認済みであるかどうかを確認してください。承認済みドメインの上限の詳細をご覧ください。

+ ドメインの追加

デベロッパーの連絡先情報

メールアドレス \*

これらのメールアドレスは、プロジェクトの変更について Google からお知らせするために使用します。

保存して次へ キャンセル

<1

4. 「スコープを追加または削除」をクリックし、スコープの追加画面を表示する。

Google Cloud Platform My First Project プロダクトとリソースの検索

API API とサービス

ダッシュボード  
ライブラリ  
認証情報  
OAuth 同意画面  
ドメインの確認  
ページの使用に関する契約

アプリ登録の編集

OAuth 同意画面 — 2 スコープ — 3 概要

スコープとは、アプリのユーザーに許可を求める権限を表します。スコープを定めることで、プロジェクトからユーザーの Google アカウントにある特定の種類のプライベートなユーザーデータへのアクセスが可能になります。 [詳細](#)

スコープを追加または削除

非機密のスコープ

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

5. Gmail API の「Gmail のすべてのメールの閲覧、作成、送信、完全な削除」を選択する。Gmail で SMTP プロトコルを直接操作する場合は、この制限付きのスコープが必須になる。

× 選択したスコープの更新

以下に一覧表示されるのは、有効な API のスコープのみです。表示されていないスコープをこの画面に追加するには、[Google API ライブラリ](#)で API を確認して有効にするか、以下の [スコープの貼り付け] テキストボックスを使用します。ページを更新すると、ライブラリから有効にしたすべての新しい API が表示されます。

フィルタ プロパティ名または値を入力

| API ↑   | 範囲   | ユーザー向けの説明                                     |
|---|--|---|
| <input type="checkbox"/> Cloud Trace API      | .../auth/trace.readonly                      | プロジェクトまたはアプリケーションのトレースデータの読み取り                |
| <input type="checkbox"/> Cloud Trace API      | .../auth/trace.append                        | プロジェクトまたはアプリケーションのトレースデータの書き込み                |
| <input checked="" type="checkbox"/> Gmail API | https://mail.google.com/                     | Gmail のすべてのメールの閲覧、作成、送信、完全な削除                 |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.modify                        | Gmail アカウントのメールの閲覧、作成、送信                      |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.compose                       | 下書きの管理とメールの送信                                 |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.addons.current.action.compose | アドオン操作時の下書きの管理とメールの送信                         |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.addons.current.message.action | アドオンの操作時にメール メッセージを表示                         |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.readonly                      | メール メッセージと設定の表示                               |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.metadata                      | ラベル、ヘッダーなど、メール メッセージのメタデータの表示 (メール本文は表示されません) |
| <input type="checkbox"/> Gmail API            | .../auth/gmail.insert                        | Gmail のメールボックスへのメールの追加                        |

ページあたりの行数: 10 21 - 30 / 39

## 6. 更新を実行する。

|                          |           |                         |   |
|--------------------------|-----------|-------------------------|---|
| <input type="checkbox"/> | Gmail API | .../auth/gmail.readonly | メール メッセージと設定の表示                               |
| <input type="checkbox"/> | Gmail API | .../auth/gmail.metadata | ラベル、ヘッダーなど、メール メッセージのメタデータの表示 (メール本文は表示されません) |
| <input type="checkbox"/> | Gmail API | .../auth/gmail.insert   | Gmail のメールボックスへのメールの追加                        |

ページあたりの行数: 10 ▼ 21 - 30 / 39 < >

### スコープの手動追加

追加したいスコープが上のテーブルに表示されない場合は、ここから入力することができます。各スコープは別の行に入力するか、カンマで区切って入力する必要があります。スコープの文字列全体 (「https://」で始まる) を指定してください。完了したら、[テーブルに追加] をクリックします。

テーブルに追加

更新

## 7. 制限付きのスコープに追加されていることを確認し、「保存して次へ」を実行する。

### 非機密のスコープ

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

### 🔒 機密性の高いスコープ

機密性の高いスコープとは、プライベート ユーザーデータへのアクセスをリクエストするスコープです。

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

### 🔒 制限付きのスコープ

制限付きのスコープとは、機密性の高いユーザーデータへのアクセスをリクエストするスコープです。

#### Gmail のスコープ

| API ↑ | 範囲           | ユーザー向けの説明          |   |
|-------|--------------|--------------------|---|
| Gmail | https://mail | Gmail のすべてのメールの閲覧、 | 🗑 |
| API   | .google.com/ | 作成、送信、完全な削除        |   |

保存して次へ

キャンセル

8. User Type で「外部」を選択した場合のみの設定である。テストユーザーを追加し、「保存して次へ」を実行する。ここで追加したユーザーのみがリソースへアクセスできるようになる。

「内部」を選択している場合は、この設定は不要。

## アプリ登録の編集

✓ OAuth 同意画面 — ✓ スcope — 3 テストユーザー — 4 概要

### テストユーザー

公開ステータスが「テスト中」に設定されている間は、テストユーザーのみがアプリにアクセスできます。アプリの確認前の許可済みユーザー数の上限は 100 で、この上限はアプリの全期間でカウントされます。 [詳細](#)

+ ADD USERS

≡ フィルタ プロパティ名または値を入力



| ユーザー情報      |  |
|-------------|--|
| @gmail.com  |  |
| l@gmail.com |  |
|             |  |

保存して次へ

キャンセル

9. 入力した内容に間違いがないか確認し、「ダッシュボードに戻る」を実行する。修正したい場合は「編集」を選択する。

Google Cloud Platform

My First Project

プロダクトとリソースの検索

API

API とサービス

ダッシュボード

ライブラリ

認証情報

OAuth 同意画面

ドメインの確認

ページの使用に関する契約

アプリ登録の編集

OAuth 同意画面 — スcope — 3 概要

OAuth 同意画面

編集

ユーザーの種類

内部

アプリ名

Blue Moon

サポートメール

アプリのロゴ

[アプリケーション ホームページ] リンク

https://symmetry-soft.com/index.htm

[アプリケーション プライバシー ポリシー] リンク

https://symmetry-soft.com/html/symmetry\_soft.htm#privacy

[アプリケーション 利用規約] リンク

https://symmetry-soft.com/software/blue\_moon/html/prod\_bluemoon.htm#licence

承認済みドメイン

連絡先メールアドレス

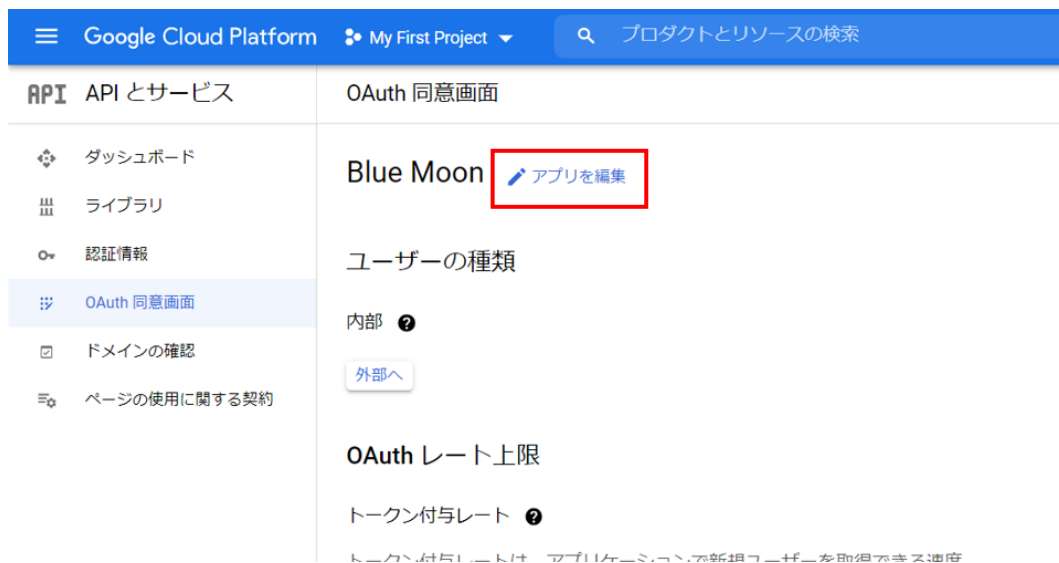
スコープ

編集

| API       | 範囲                       | ユーザー向けの説明                     |
|-----------|--------------------------|-------------------------------|
| Gmail API | https://mail.google.com/ | Gmail のすべてのメールの閲覧、作成、送信、完全な削除 |

ダッシュボードに戻る

10. 後から修正を行う場合は、「アプリを編集」を実行する。



#### 認証情報

11. メニューから「認証情報」を選択し、「認証情報を作成」を実行する。



12. プルダウンリストから「OAuth クライアント ID」を選択する。

The screenshot shows the Google Cloud Platform console interface. At the top, there's a blue header with 'My First Project' and a search bar. Below the header, the 'Authentication' section is active, showing options to '+ 認証情報を作成' (Create authentication info) and '削除' (Delete). A dropdown menu is open, listing several authentication methods: 'API キー' (API key), 'OAuth クライアント ID' (highlighted with a red box), 'サービス アカウント' (Service account), and 'ウィザードで選択' (Select with wizard). The 'OAuth クライアント ID' option is described as 'ユーザーのデータにアクセスできるようにユーザーの同意をリクエストします' (Requests user consent so you can access user data). Below the dropdown, there's a table with columns for '名前' (Name), '作成日' (Created), and '種類' (Type). The table is currently empty, with a message '表示する OAuth クライアントがありません' (No OAuth clients to display).

13. 名前に適当な任意の名称を入力し、「作成」を実行する。

The screenshot shows the 'OAuth クライアント ID の作成' (Create OAuth client ID) page in the Google Cloud Platform console. The left sidebar shows the 'API とサービス' (APIs & Services) section, with '認証情報' (Authentication) selected. The main content area has a heading 'OAuth クライアント ID の作成' and a description of client IDs. Below the description, there's a dropdown menu for 'アプリケーションの種類' (Application type) set to 'デスクトップ アプリ' (Desktop app). The '名前' (Name) field is filled with 'デスクトップ クライアント: Blue Moon' and is highlighted with a red box. Below the name field, there's a note: 'OAuth 2.0 クライアントの名前。この名前はコンソールでクライアントを識別するためにのみ使用され、エンドユーザーには表示されません。' (OAuth 2.0 client name. This name is used only to identify the client in the console and is not displayed to end users). At the bottom, there are two buttons: '作成' (Create) and 'キャンセル' (Cancel). The '作成' button is highlighted with a red box.

14. 作成した「クライアント ID」と「クライアント・シークレット」は、Blue Moon の設定画面で資格情報ファイルの作成時に必要になる。この画面で値をコピーし控えておくか、認証情報を選択して後から再度表示することもできる。

## OAuth クライアントを作成しました

クライアント ID とシークレットには、常に API とサービスの認証情報からアクセスできます



[OAuth 同意画面](#)が公開および確認されるまで、OAuth アクセスは組織内のユーザーに制限されます

クライアント ID

[Redacted Client ID]



クライアント シークレット

[Redacted Client Secret]



↓ JSON をダウンロード

OK

クライアント・シークレットは、非公開とする資格情報です。ただし、第三者に漏洩した場合でも OAuth の仕様上、他人のリソースへアクセスすることは非常に困難です。そのため、漏洩させないことは大切ですが、パスワードの様に神経質になる必要はありません。

内部アプリとして登録し、アクセスできるユーザーを制限かつ監査ログをチェックするほうが効率的な安全対策となります。



#### 4. Microsoft 365 (Exchange Online)

アプリの登録や設定を行うには、Microsoft 365 と紐づいたアカウントで管理できる Azure Portal の Azure AD(Active Directory)を使用します。

Microsoft 365 を契約していない Microsoft アカウント (outlook.com 等) で管理する個人ユーザーの場合も、同様に Azure Portal を使用します。

アプリを使用するために必要な設定作業の大まかな流れは、次のようになります。

- ① [アプリの登録](#)
- ② [ユーザーやグループをアプリに割り当てる](#)
- ③ [アクセス許可（管理者の同意）の付与](#)
- ④ [SMTP AUTH の有効化](#)

なお、デスクトップアプリの場合は、クライアント・シークレットは使用できません。そのため、クライアント・シークレットの作成作業は不要です。

## 登録手順

Azure Portal 上には、アプリを登録するサブスクリプションが既に存在していることを前提に説明します。存在していない場合は作成して下さい。

### アプリの登録

1. メニューから「Azure Active Directory」を選択する。

The screenshot shows the Azure Portal interface. On the left is a navigation menu with various options. The 'Azure Active Directory' option is highlighted with a red rectangle. The main content area displays a welcome message 'Azure へようこそ!' and several service tiles. The 'Azure の無料試用版から開始する' tile is prominent, along with 'Azure Active Directory' and 'Azure サービス'.

**Azure へようこそ!**  
サブスクリプションをお持ちでない場合は、次のオプションをご確認ください。

**Azure の無料試用版から開始する**  
Azure の製品とサービスに使用できる 200 ドルの無料クレジットを取得できるだけでなく、人気の無料サービスを 12 か月間利用できます。  
[開始](#) [詳細情報](#)

**Azure Active Directory**  
Azure Active Directory をスマート ポリシーを設定する。  
[表示](#) [詳細情報](#)

**Azure サービス**

[リソースの作成](#) [クイックスタートセン...](#) [Virtual Machines](#) [App Service](#) [ストレージアカウント](#)

**移動**

2. Azure AD のメニューから「アプリの登録」を選択し、「新規登録」実行する。



3. アプリケーションの登録ページで次の様に各項目を入力し、完了後「登録」を実行する。

#### アプリ情報

| 項目名               | 入力値                                  |
|-------------------|--------------------------------------|
| 名前                | Blue Moon                            |
| サポートされているアカウントの種類 | この組織ディレクトリのみに含まれるアカウント（シングルテナント） ※ 1 |
| リダイレクト URI        | このページでは何も指定しない。（後で設定する）              |

※ 1） Microsoft アカウント（outlook.com 等）で管理する個人ユーザーの場合は、個人の Microsoft アカウントをサポートするマルチテナントを選択する。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Symmetry Soft >

## アプリケーションの登録

\* 名前

このアプリケーションのユーザー向け表示名 (後で変更できます)。

Blue Moon

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

☒ この組織ディレクトリのみに含まれるアカウント (Symmetry Soft のみ - シングル テナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype、Xbox など)

☐ 個人用 Microsoft アカウントのみ

[選択に関する詳細...](#)

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

パブリック クライアント/ネ... 例: myapp://auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加

[続行すると、Microsoft プラットフォーム ポリシーに同意したことになります](#)

**登録**

4. メニューの「概要」を選択し、表示名とアプリケーション（クライアント）ID が表示されていることを確認する。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Symmetry Soft >

**Blue Moon**

検索 (Ctrl+/) << 削除 エンドポイント プレビュー機能

**概要**

クイック スタート

統合アシスタント

管理

ブランド

認証

証明書とシークレット

トークン構成

へ 基本

表示名 : Blue Moon

アプリケーション (クラ... :

オブジェクト ID :

ディレクトリ (テナント) ... :

サポートされているアカ... : 所属する組織のみ

新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変

## 認証

5. メニューから「認証」を選択し、「プラットフォームを追加」を実行する。



6. プラットフォームの構成から、「モバイルアプリケーションとデスクトップアプリケーション」を選択する。



7. デスクトップとデバイスの構成の「カスタムリダイレクト URI」に次の URI を入力する。 「<http://127.0.0.1>」

## デスクトップとデバイスの構成

×

[すべてのプラットフォーム](#)

[クイックスタート](#)

[ドキュメント](#)

### リダイレクト URI

ユーザー認証に成功した後に認証応答 (トークン) を返すときに宛先として受け入れる URI。応答 URL とも呼ばれます。 [リダイレクト URI と制限の詳細情報](#)

- ☐ <https://login.microsoftonline.com/common/oauth2/nativeclient>
- ☐ [https://login.live.com/oauth20\\_desktop.srf](https://login.live.com/oauth20_desktop.srf) (LiveSDK)
- ☐ [msal019e00f4-3c74-4495-b18b-e2e8872b1d4e://auth](https://login.live.com/msal019e00f4-3c74-4495-b18b-e2e8872b1d4e://auth) (MSAL のみ)

### カスタム リダイレクト URI

<http://127.0.0.1>



### API のアクセス許可

8. メニューから「API のアクセス許可」を選択し「アクセス許可の追加」を実行する。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Symmetry Soft > Blue Moon

## Blue Moon | API のアクセス許可

検索 (Ctrl+/) << >> 最新の情報に更新 フィードバックがある場合

概要

クイックスタート

統合アシスタント

管理

ブランド

認証

証明書とシークレット

トークン構成

**API のアクセス許可**

API の公開

アプリ ロール

所有者

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。

**+ アクセス許可の追加** Symmetry Soft に管理者の同意を与えます

| API / アクセス許可の名前     | 種類   | 説明                            |
|---------------------|------|-------------------------------|
| Microsoft Graph (1) |      |                               |
| User.Read           | 委任済み | Sign in and read user profile |

アクセス許可とユーザーの同意を表示および管理するために、[エンタープライズ アプリケー](#)

9. 「API のアクセス許可の要求」で「Microsoft API」タブの「Microsoft Graph」を選択する。

## API アクセス許可の要求


>


API を選択します


Microsoft API


所属する組織で使用している API    自分の API


よく使用される Microsoft API


**Microsoft Graph**  
Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Azure AD、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。


**Azure Service Management**  
Azure portal で利用できる機能の大部分へのプログラムによるアクセス

**Data Export Service for Microsoft Dynamics 365**  
Microsoft Dynamics CRM 組織から外部宛先にデータをエクスポートします

**Dynamics 365 Business Central**  
Dynamics 365 Business Central のデータと機能へのプログラムによるアクセス

**Dynamics CRM**  
CRM ビジネス ソフトウェアと ERP システムの機能にアクセスします

**Flow Service**  
フロー テンプレートの埋め込みとフローの管理

**Intune**  
Intune データへのプログラムによるアクセス

10. アプリケーションに必要なアクセス許可の種類で「委任されたアクセス許可」を選択する。

## API アクセス許可の要求

×

< すべての API



Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデーモンとして実行されます。

11. OpenId アクセス許可から「email」、「offline\_access」、「openid」を選択状態にする。

| アクセス許可                              |   | 管理者の同意が必要 |
|-------------------------------------|---|-----------|
| ▽ OpenId アクセス許可 (3)                 |   |           |
| <input checked="" type="checkbox"/> | email ⓘ<br>View users' email address                                    | いいえ       |
| <input checked="" type="checkbox"/> | offline_access ⓘ<br>Maintain access to data you have given it access to | いいえ       |
| <input checked="" type="checkbox"/> | openid ⓘ<br>Sign users in   | いいえ       |
| <input type="checkbox"/>            | profile ⓘ<br>View users' basic profile                                  | いいえ       |

12. Mail から「Mail.Send」、「Mail.Send.Share」を選択状態にする。

|                                     |  |     |
|-------------------------------------|--|-----|
| ▽ Mail (2)                          |  |     |
| <input type="checkbox"/>            | Mail.Read ⓘ<br>Read user mail                                  | いいえ |
| <input type="checkbox"/>            | Mail.Read.Shared ⓘ<br>Read user and shared mail                | いいえ |
| <input type="checkbox"/>            | Mail.ReadBasic ⓘ<br>Read user basic mail                       | いいえ |
| <input type="checkbox"/>            | Mail.ReadWrite ⓘ<br>Read and write access to user mail         | いいえ |
| <input type="checkbox"/>            | Mail.ReadWrite.Shared ⓘ<br>Read and write user and shared mail | いいえ |
| <input checked="" type="checkbox"/> | Mail.Send ⓘ<br>Send mail as a user                             | いいえ |
| <input checked="" type="checkbox"/> | Mail.Send.Shared ⓘ<br>Send mail on behalf of others            | いいえ |

13. SMTP から「SMTP.Send」を選択状態にする。

|                                     |  |     |
|-------------------------------------|--|-----|
| ▽ SMTP (1)                          |  |     |
| <input checked="" type="checkbox"/> | SMTP.Send ⓘ<br>Send emails from mailboxes using SMTP AUTH. | いいえ |

14. User から「User.Read」を選択状態にする。(既定で選択状態になっている)



|                                     |   |     |
|-------------------------------------|---|-----|
| ▼ User (1)                          |   |     |
| <input type="checkbox"/>            | User.Export.All ⓘ<br>Export user's data                     | はい  |
| <input type="checkbox"/>            | User.Invite.All ⓘ<br>Invite guest users to the organization | はい  |
| <input type="checkbox"/>            | User.ManageIdentities.All ⓘ<br>Manage user identities       | はい  |
| <input checked="" type="checkbox"/> | User.Read ⓘ<br>Sign in and read user profile                | いいえ |
| <input type="checkbox"/>            | User.Read.All ⓘ<br>Read all users' full profiles            | はい  |
| <input type="checkbox"/>            | User.ReadBasic.All ⓘ<br>Read all users' basic profiles      | いいえ |

15. 選択完了後に「アクセス許可の追加」を実行する。

|                          |   |
|--------------------------|---|
| <input type="checkbox"/> | User.ReadWrite ⓘ<br>Read and write access to user profile       |
| <input type="checkbox"/> | User.ReadWrite.All ⓘ<br>Read and write all users' full profiles |

アクセス許可の追加

破棄

16. 次の画像の様に選択した七つの API が表示されていることを確認する。

#### 構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加    ✓ Symmetry Soft に管理者の同意を与えます

| API / アクセス許可の名前       | 種類   | 説明  | 管理者の同意が必要 | 状態 |
|-----------------------|------|---|-----------|----|
| ▼ Microsoft Graph (7) |      |   |           |    |
| email                 | 委任済み | View users' email address                           | いいえ       |    |
| Mail.Send             | 委任済み | Send mail as a user                                 | いいえ       |    |
| Mail.Send.Shared      | 委任済み | Send mail on behalf of others                       | いいえ       |    |
| offline_access        | 委任済み | Maintain access to data you have given it access to | いいえ       |    |
| openid                | 委任済み | Sign users in                                       | いいえ       |    |
| SMTP.Send             | 委任済み | Send emails from mailboxes using SMTP AUTH.         | いいえ       |    |
| User.Read             | 委任済み | Sign in and read user profile                       | いいえ       |    |

## ブランドの設定

17. メニューから「ブランド」を選択し、次の様に各項目を入力する。入力完了後に「保存」を実行する。

| 項目名               | 入力値   |
|-------------------|---|
| 名前                | Blue Moon   |
| ロゴ                | BlueMoonLogo215.png ※1  |
| ホームページ URL        | <a href="https://symmetry-soft.com/">https://symmetry-soft.com/</a>   |
| サービス利用規約 URL      | <a href="https://symmetry-soft.com/software/blue_moon/html/prod_bluemoon.htm#licence">https://symmetry-soft.com/software/blue_moon/html/prod_bluemoon.htm#licence</a> |
| プライバシーに関する声明の URL | <a href="https://symmetry-soft.com/html/symmetry_soft.htm#privacy">https://symmetry-soft.com/html/symmetry_soft.htm#privacy</a>                                       |
| パブリッシャードメイン       | 任意のドメイン   |
| 発行元の検証            | MPN ID は、所有している場合に追加する。組織内の内部アプリとして使用する場合は、追加しなくても問題無い。   |

※1) アプリロゴのダウンロード URL

[https://symmetry-soft.com/software/blue\\_moon/download/logos/logos.htm](https://symmetry-soft.com/software/blue_moon/download/logos/logos.htm)

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Symmetry Soft > Blue Moon

Blue Moon | ブランド

検索 (Ctrl+)

保存

破棄

フィードバックがある場合

概要

クイックスタート

統合アシスタント

管理

ブランド

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者 | プレビュー

マニフェスト

サポート + トラブルシューティング

トラブルシューティング

新しいサポート リクエスト

名前 \*

Blue Moon

ロゴ



新しいロゴのアップロード

ファイルの選択

ホームページ URL

<https://symmetry-soft.com/>

サービス利用規約 URL

[https://symmetry-soft.com/software/blue\\_moon/html/prod\\_bluemoon.htm#licence](https://symmetry-soft.com/software/blue_moon/html/prod_bluemoon.htm#licence)

プライバシーに関する声明の URL

[https://symmetry-soft.com/html/symmetry\\_soft.htm#privacy](https://symmetry-soft.com/html/symmetry_soft.htm#privacy)

パブリッシャー ドメイン

symmetry-soft.net

ドメインを更新します

発行元の検証

検証済みの Microsoft パートナー センター (MPN) アカウントをアプリケーションに関連付けます。検証済みのバッジは、アプリケーションの同意画面など、さまざまな場所に表示されます。 [詳細情報](#)

MPN ID

MPN ID を追加して発行元を確認します

発行元の表示名

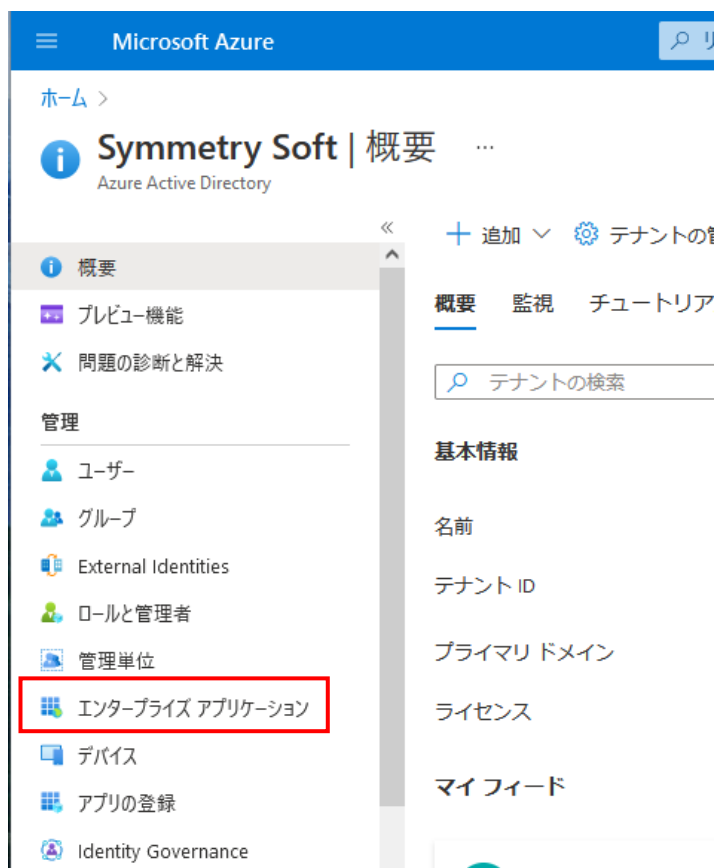
未指定

ユーザーやグループにアプリを割り当てる

アプリにアクセスできるユーザーを割り当てる必要があります。グループ単位でも割り当て可能です。ただし、グループベースの割り当ては、Azure AD Premium P1 or P2 エディションを契約する必要があります。ここでは、ユーザーベースの割り当て手順を説明します。

なお、Microsoft アカウント（outlook.com 等）で管理する個人ユーザーの場合は、この設定は不要です。

1. メニューから「Active Directory」を選択する。
2. Active Directory のメニューから、「エンタープライズ アプリケーション」を選択する。



3. アプリ一覧から Blue Moon を選択する。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Symmetry Soft > エンタープライズ アプリケーション

## エンタープライズ アプリケーション | すべてのアプリケーション

Symmetry Soft - Azure Active Directory

概要

- 概要
- 問題の診断と解決

管理

- すべてのアプリケーション
- アプリケーション プロキシ
- ユーザー設定

セキュリティ

- 条件付きアクセス
- 同意とアクセス許可

アクティビティ

- サインイン ログ
- 使用状況と分析情報
- 監査ログ
- プロビジョニング ログ
- アクセス レビュー
- 管理者の同意要求

新しいアプリケーション | 列 | プレビュー機能 | フィードバックがある場合

新しいエンタープライズ アプリ検索のプレビューをお試しください。クリックするとプレビューが有効になります。 →

アプリケーションの種類: エンタープライズ アプリ... | アプリケーションの状態: すべて | アプリケーションの可視性: すべて

最初の 50 件が表示されています。すべてのアプリケーションを検索するには、表示名またはアプリケーション ID を入力してください。

| 名前                           | ホームページ URL                              |
|------------------------------|---|
| Blue Moon                    | https://symmetry-soft.com/              |
| Common Data Service          | http://www.microsoft.com/dynamics/crm   |
| Microsoft Teams              |   |
| Office 365 Exchange Online   | http://office.microsoft.com/outlook/    |
| Office 365 Management APIs   |   |
| Office 365 SharePoint Online | http://office.microsoft.com/sharepoint/ |
| Office 365 Yammer            | https://products.office.com/yammer/     |
| Outlook Groups               |   |
| Power BI Service             |   |
| Skype for Business Online    |   |

4. メニューから「プロパティ」を選択する。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Symmetry Soft > エンタープライズ アプリケーション >

## Blue Moon | 概要

エンタープライズ アプリケーション

概要

- 概要
- デプロイ計画

管理

- プロパティ
- 所有者
- ロールと管理者 (プレビュー)
- ユーザーとグループ
- シングル サインオン
- プロビジョニング
- アプリケーション プロキシ
- セルフサービス

セキュリティ

- 条件付きアクセス

### プロパティ

名前 ①  
Blue Moon

アプリケーション ID ①  
...

オブジェクト ID ①  
...

### Getting Started

1. ユーザーとグループの割り当て  
特定のユーザーおよびグループにアプリケーションへのアクセスを付与  
[ユーザーとグループの割り当て](#)

5. 「ユーザーのサインインが有効になっていますか？」で「はい」を選択し、「保存」を実行する。

Microsoft Azure

ホーム > Blue Moon

Blue Moon | プロパティ ...

エンタープライズ アプリケーション

概要  
デプロイ計画  
管理  
プロパティ  
所有者  
ロールと管理者 (プレビュー)  
ユーザーとグループ  
シングル サインオン

保存 破棄 削除 フィードバックがある場合

ユーザーのサインインが有効になっていますか? ①

はい いいえ

名前 \* ① Blue Moon

ホームページ URL ① https://symmetry-soft.com/

ロゴ ①

ファイルの選択

6. メニューから「ユーザーとグループ」を選択し、「ユーザーまたはグループの追加」を実行する。

Microsoft Azure

ホーム > Blue Moon

Blue Moon | ユーザーとグループ ...

エンタープライズ アプリケーション

概要  
デプロイ計画  
管理  
プロパティ  
所有者  
ロールと管理者 (プレビュー)  
ユーザーとグループ  
シングル サインオン  
プロビジョニング  
アプリケーション プロキシ

+ ユーザーまたはグループの追加 編集 削除

アプリケーションは、割り当てられたユーザーのマイ アプリ内に

最初の 200 件を表示しています。すべてのユーザーとグループ

表示名

アプリケーションの割り当てが見つかりませんでした

7. 「ユーザー」を選択しリストから割り当てるユーザーを選択状態にする。選択完了後に「選択」を実行する。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > Blue Moon >

### 割り当ての追加

Symmetry Soft

お客様の Active Directory プランレベルでは、グループを割り当てるできません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

選択されていません

ロールを選択してください

Default Access

割り当て

ユーザー

検索

選択済み

選択したアイテム

選択

ユーザーを選択した場合は、自動的に「既定のロール」が割り当てられる。  
ロールの選択がサポートされている場合は、ロールの割り当てが可能となる。

8. 割り当てたユーザー数が正しいことを確認し、「割り当て」を実行する。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > Blue Moon >

### 割り当ての追加

Symmetry Soft

お客様の Active Directory プランレベルでは、グループを割り当てることはできません。

ユーザー

1 人のユーザーが選択されました。

ロールを選択してください

Default Access

割り当て

9. 割り当てに成功すると、「ユーザーとグループ」に選択したユーザーが表示される。

The screenshot shows the Microsoft Azure portal interface. At the top, the header bar displays 'Microsoft Azure' and a search bar. Below the header, the breadcrumb trail shows 'ホーム > Blue Moon'. The main heading is 'Blue Moon | ユーザーとグループ ...' with the subtitle 'エンタープライズ アプリケーション'. The left sidebar contains a navigation menu with items: '概要', 'デプロイ計画', '管理', 'プロパティ', '所有者', 'ロールと管理者 (プレビュー)', 'ユーザーとグループ' (highlighted with a red box), 'シングル サインオン', and 'プロビジョニング'. The main content area shows a list of users. At the top of the list, there are buttons: '+ ユーザーまたはグループの追加', '編集', '削除', and '資格'. Below these is an information box stating 'アプリケーションは、割り当てられたユーザーのマイ アプリ内に表'. A search bar indicates '最初の 200 件を表示しています。すべてのユーザーとグループを'. The list has a header '表示名'. The first two rows of the list are highlighted with a red box, showing user avatars and names.

| 表示名                      |          |
|--------------------------|----------|
| <input type="checkbox"/> | [Avatar] |
| <input type="checkbox"/> | [Avatar] |

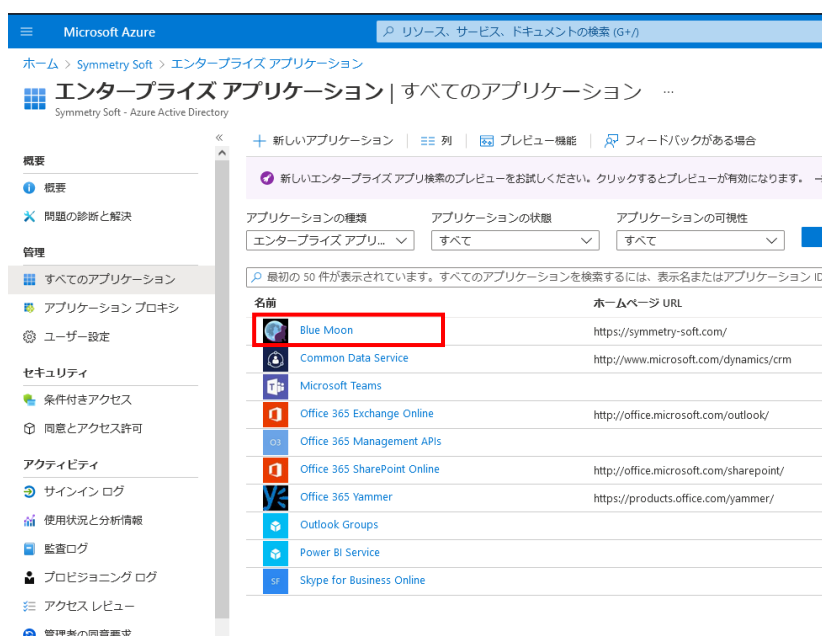
アクセス許可（管理者の同意）の付与

管理者の同意を付与することで、ユーザーがサインイン時に行うリソースへのアクセス承認作業を省略できます。（サインインのみで完了する）

内部アプリ（シングルテナント）として管理する場合は、この管理者の同意設定が必須になります。

なお、Microsoft アカウント（outlook.com 等）で管理する個人ユーザーの場合は、この設定は不要です。

1. Active Directory のメニューで「エンタープライズ アプリケーション」を選択し、一覧から「Blue Moon」を選択する。





2. メニューから「アクセス許可」を選択し、「〇〇〇に管理者の同意を与える」を実行する。

Microsoft Azure

ホーム > Symmetry Soft > Blue Moon > Blue Moon

Blue Moon | アクセス許可 ...

更新 ✓ アクセス許可の確認 フィードバックがある場合

アクセス許可

ご使用のテナントに対するアクセス許可をアプリケーションに付与できます。そのために必要なのは、管理者がすべてのユーザーか（ユーザーの同意）、または管理者がアプリケーションを統合してセルフサービス アクセスを有効にしたり、ユーザーを付与できます。これにより、エンド ユーザーはアプリケーションを使用するときに同意を求められることがなくなります。管理者はこのテナント内のすべてのユーザーに代わって同意を付与できます。これにより、エンド ユーザーはアプリケーションシミュレーションします。

Symmetry Soft に管理者の同意を与えます

管理者の同意 ユーザーの同意

アクセス許可の検索

| API 名           | 権限  |
|-----------------|---|
| Microsoft Graph |   |
| Microsoft Graph | Maintain access to data you have given it access to |
| Microsoft Graph | Send mail on behalf of others                       |
| Microsoft Graph | Sign in and read user profile                       |

### 割り当ての確認

ユーザー毎に割り当てたアプリは、次の方法で確認できます。

なお、Microsoft アカウント（outlook.com 等）で管理する個人ユーザーの場合は、この設定は不要です。

1. Active Directory のメニューで「ユーザー」を選択する。
2. ユーザー一覧からアプリを割り当てたユーザーを選択する。
3. メニューから「アプリケーション」を選択すると、割り当て済みのアプリが表示される。

Microsoft Azure

ホーム > Symmetry Soft > ユーザー > 堀咲 翔子

ユーザー | アプリケーション ...

直接の割り当て、継承された割り当て、またはユーザーが承諾した割り当ては最大 1,000 件表示されます。表示されるテキストで検索

| 名前        | ロール     | 割り当て     |
|-----------|---------|----------|
| Blue Moon | 既定のアクセス | 直接割り当て済み |

アプリケーション

アクセス許可（管理者の同意）の取り消し  
管理者の同意を取り消したい場合は次の様に行います。

1. Active Directory のメニューで「アプリの登録」を選択し、一覧から「Blue Moon」を選択する。
2. メニューから「API のアクセス許可」を選択し、API のカテゴリまたは API 毎に右端のメニューを選択し取り消す。

ホーム > Symmetry Soft > Blue Moon

Blue Moon | API のアクセス許可 ✕ ...

検索 (Ctrl+F) << 最新の情報に更新 | フィードバックがある場合

概要

クイックスタート

統合アシスタント

管理

ブランド

認証

証明書とシークレット

!!! トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者 | プレビュー

マニフェスト

サポート + トラブルシューティング

トラブルシューティング

...

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ✓ Symmetry Soft に管理者の同意を与えます

| API / アクセス許可の名前       | 種類   | 説明  | 管理者の同意が必要 | 状態                      |     |
|-----------------------|------|---|-----------|-------------------------|-----|
| ▼ Microsoft Graph (7) |      |   |           |                         |     |
| email                 | 委任済み | View users' email address                           | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| Mail.Send             | 委任済み | Send mail as a user                                 | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| Mail.Send.Shared      | 委任済み | Send mail on behalf of others                       | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| offline_access        | 委任済み | Maintain access to data you have given it access to | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| openid                | 委任済み | Sign users in                                       | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| SMTP.Send             | 委任済み | Send emails from mailboxes using SMTP AUTH.         | いいえ       | ✓ Symmetry Soft に付与さ... | ... |
| User.Read             | 委任済み | Sign in and read user profile                       | いいえ       | ✓ Symmetry Soft に付与さ... | ... |

アクセス許可の削除  
管理者の同意を取り消す

## SMTP AUTH の有効化

Blue Moon から SMTP 送信を可能にするためには、アプリを使用するユーザー毎に SMTP AUTH 認証を有効化する必要があります。既定の状態ではこの設定は無効化されています。この設定を有効化にしない場合は、OAuth 認証で取得したアクセストークンを使用した SMTP AUTH 認証時に、Exchange Online から認証を拒否されるので注意して下さい。

なお、Microsoft アカウント（outlook.com 等）で管理する個人ユーザーの場合は、この設定は不要です。

1. Microsoft 365 管理センターに管理ユーザーとしてサインインする。
2. メニューの「ユーザー」から「アクティブなユーザー」を選択する。



3. ユーザーリストから SMTP AUTH を有効化するユーザーを選択する。

Microsoft 365 管理センター

ホーム > アクティブなユーザー

## アクティブなユーザー

推奨処置 (2)

ユーザーの追加 ユーザー テンプレート 複数のユーザーを追加 多要素認証

| 表示名 ↑ | ユーザー名 |
|-------|-------|
|       |       |
|       |       |

4. 「メール」タブを選択し「メールアプリを管理する」を実行する。

🔄 ×

  [パスワードのリセット](#) [サインインをブロック](#) ...

[写真の変更](#)

アカウント デバイス ライセンスとアプリ **メール** OneDrive

メールボックス アクセス許可

メール アプリ

POP がブロックされました  
OWA がブロックされました  
IMAP がブロックされました  
その他のメール アプリは許可されています

[メール アプリを管理する](#)

グローバル アドレス一覧に表示する  
はい

メールの転送  
なし

グローバル アドレス一覧の表示設定  
を管理する

メールの転送を管理する

自動応答  
オン

その他の処理  
共有メールボックスに変換する  
Exchange のプロ

[自動応答を管理する](#)

[Help & support](#)

5. 「認証済み SMTP」を選択し、「変更の保存」を実行する。



## メール アプリを管理する

堀咲 翔子 が Microsoft 365 のメールにアクセスできるアプリを選びます。

- ☐ Outlook on the web
- ☐ Outlook デスクトップ (MAPI)
- ☐ Exchange Web サービス
- ☐ モバイル (Exchange ActiveSync)
- ☐ IMAP
- ☐ POP

☒ 認証済み SMTP



変更の保存

6. 上記有効化の作業を、必要なユーザー毎に繰り返して下さい。

#### 注意点

Microsoft 365 を契約していない個人ユーザーが、個人用アカウント(outlook.com 等)で管理する場合の注意点を記載します。

Microsoft 365 を契約しているユーザーの場合は不要です。

接続時にエラーが発生する場合は、次の設定を行って下さい。

Blue Moon の「送信設定」 > 「SMTP over SSL/TLS の使用」 > 「詳細設定」で、「クライアント証明書を使用する」のチェックを OFF にする。

暗号化通信の詳細設定

×

SSL/TLSタイプ

受信 TLS 1.0

送信 STARTTLS(TLS 1.2)

証明書関連

☐ クライアント証明書を使用する

...

☒ リモート証明書を検証する

OK

キャンセル

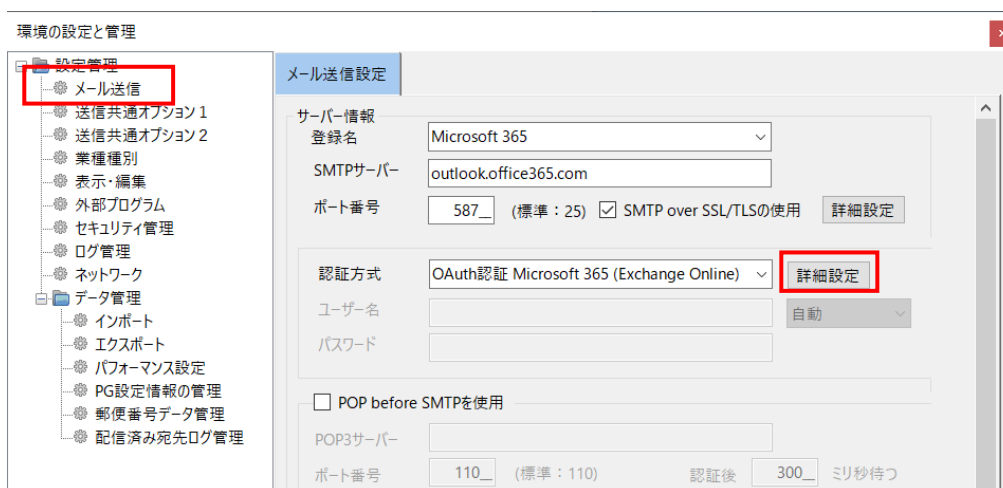
## 5. 資格情報ファイルの作成

Blue Moon にクライアント ID やクライアント・シークレット等の資格情報 (Credential) を設定するための、資格情報ファイルの作成方法について説明します。

資格情報ファイルを使用することで Blue Moon を使用するユーザーは、このファイルをインポートするだけで OAuth 認証設定を行うことができます。また、このファイルは暗号化されているため、ユーザーに資格情報の詳細を知らせる必要もなくなります。

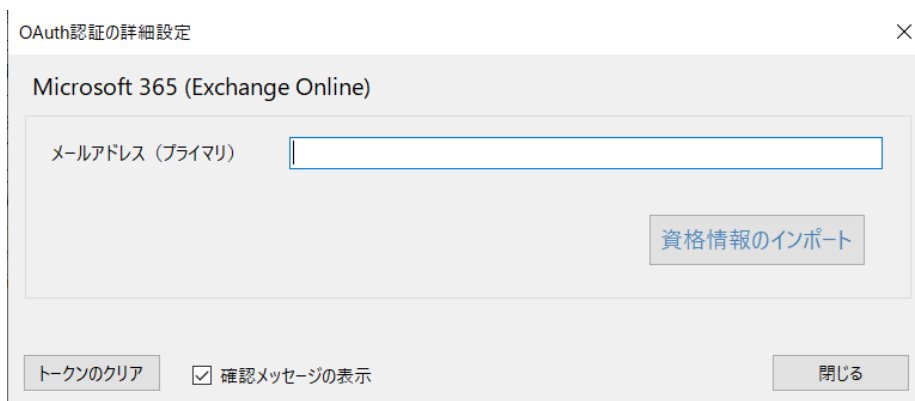
資格情報ファイル作成画面の表示

1. 事前に Blue Moon の「環境の設定と管理」画面の「メール送信」タブで、OAuth 認証を行うサーバー情報を登録しておいて下さい。
2. 認証方式は、Google Workspace か Microsoft 365 を選択し、「詳細設定」ボタンをクリックして下さい。



3. OAuth 認証の詳細設定画面の表示後、次のキーを同時に押して下さい。

**「Ctrl + Shift + Alt + 9」**



4. 次の様に資格情報ファイルの作成領域が表示されます。

OAuth認証の詳細設定 ×

Microsoft 365 (Exchange Online)

メールアドレス（プライマリ）

テナント

クライアントID

クライアント・シークレット

認可エンドポイント

認可スコープ

トークン取得エンドポイント

トークン取得スコープ

☒ 確認メッセージの表示

元に戻す場合は、再度「**Ctrl + Shift + Alt + 9**」を押すか、または「閉じる」ボタンをクリックし一旦画面を閉じた後で、再度「詳細設定」ボタンをクリックして再表示して下さい。

#### 機能の説明

各機能について説明します。

##### 1. テナント

Microsoft 365 を利用する場合にのみ設定可能になる項目です。

内部アプリとして管理する場合に、リソースへアクセスできるアカウントの種類に応じて選択する必要があります。ここで選択したテナントは、認可エンドポイントとトークン取得エンドポイントの次のテナント部分を置き換えます。通常は既定値の「organizations」を選択して下さい。

<https://login.microsoftonline.com/{テナント}/oauth2/v2.0/authorize>

<https://login.microsoftonline.com/{テナント}/oauth2/v2.0/token>



テナントの種類とサインイン可能なアカウントの関係は次のようになります。

- **common:** 個人の Microsoft アカウントと Azure AD の職場/学校アカウント
- **organizations (既定値):** Azure AD の職場/学校アカウント
- **consumers:** 個人の Microsoft アカウント (MSA)
- **contoso.onmicrosoft.com:** 特定の Azure AD テナントの職場/学校アカウント

なお、Microsoft 365 を契約していない Microsoft アカウント (outlook.com 等) で管理する個人ユーザーの場合は、「common」を選択して下さい。

## 2. クライアント ID

登録しているアプリを識別するための ID です。アプリの登録時に発行される ID で、認可コードやアクセストークンの取得時に必要になります。(必須項目)

## 3. クライアント・シークレット

「認可コード、アクセストークン、リフレッシュトークン」と「クライアント ID」との整合性検証に用いる値の一つです。アクセストークンの取得時に必要になります。非公開とする値ですが、外部に漏洩した場合でも第三者が他人のリソースへ簡単にアクセスすることが困難となる仕組みが OAuth 認証のメリットの一つです。また、内部アプリとして登録することで、第三者が不正にサインインした場合でも監査ログで検出することが可能になります。

Google Workspace では必須項目ですが、Microsoft 365 の場合は不要です。

## 4. 認可エンドポイント

認可コードを取得する際に接続するサーバーの URI を指定します。

通常は規定値を変更しないで下さい。(必須項目)

## 5. 認可スコープ

認可コードを取得する際にサーバーへ送る、OpenID Connect とリソースへのアクセス権の範囲を指定します。

通常は規定値を変更しないで下さい。(必須項目)

## 6. トークン取得エンドポイント

アクセストークンを取得する際に接続するサーバーの URI を指定します。

通常は規定値を変更しないで下さい。(必須項目)

7. トークン取得スコープ

アクセストークンを取得する際にサーバーへ送る、リソースへのアクセス権の範囲を指定します。

通常は規定値を変更しないで下さい。(必須項目)

8. 既定値の設定ボタン

指定した OAuth 認証プロバイダ毎に最適化された既定値を、各項目に自動設定します。既定値が設定された項目に関しては、特別な事情がない限り変更しないようにして下さい。間違った情報を設定した場合は、OAuth 認証による接続ができなくなるので注意して下さい。

なお、OAuth 認証時に指定するパラメータで、各プロバイダで共通となる重要な項目 (**state**, **code\_challenge**, **code\_verifier** 等) に関しては、プログラム内で設定しているためここでの設定は不要です。

9. 資格情報ファイルの作成ボタン

このボタンをクリックすることで、資格情報ファイルを任意のフォルダに作成します。このボタンをクリックする前に、必須項目は全て入力するようにして下さい。

作成手順

資格情報ファイルの作成手順について説明します。

1. 「規定値の設定」ボタンをクリックして下さい。各項目に規定値が自動的に設定されます。特別な事情が無い限り、規定値からの変更は不要です。

|               |  |
|---------------|--|
| テナント          | <input type="text" value="organizations"/>   |
| クライアントID      | <input type="text"/>   |
| クライアント・シークレット | <input type="text"/>   |
| 認可エンドポイント     | <input type="text" value="https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize"/> |
| 認可スコープ        | <input type="text" value="https://outlook.office.com/SMTPSend offline_access"/>                    |
| トークン取得エンドポイント | <input type="text" value="https://login.microsoftonline.com/organizations/oauth2/v2.0/token"/>     |
| トークン取得スコープ    | <input type="text" value="https://outlook.office.com/SMTPSend"/>                                   |

2. Microsoft 365 を指定している場合は、アクセスするアカウントの種類に応じてテナントを指定してください。
3. 「クライアント ID」と「クライアント・シークレット」を入力して下さい。  
Microsoft 365 を指定している場合は、「クライアント・シークレット」の入力は不要です。
4. 「資格情報ファイルの作成」ボタンをクリックし、ファイルを作成して下さい。  
OAuth 認証を利用するユーザーにここで作成したファイルを配布しインポートして貰います。

|               |  |
|---------------|--|
| テナント          | <input type="text" value="organizations"/>   |
| クライアントID      | <input type="text" value="*****"/>   |
| クライアント・シークレット | <input type="text"/>   |
| 認可エンドポイント     | <input type="text" value="https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize"/> |
| 認可スコープ        | <input type="text" value="https://outlook.office.com/SMTPSend offline_access"/>                    |
| トークン取得エンドポイント | <input type="text" value="https://login.microsoftonline.com/organizations/oauth2/v2.0/token"/>     |
| トークン取得スコープ    | <input type="text" value="https://outlook.office.com/SMTPSend"/>                                   |

インポートの方法等に関しては、ヘルプマニュアルの「設定管理」>「環境の設定と管理」>「メール送信設定」の「9. 詳細設定（OAuth 認証）」を参照して下さい。

## 6. 注意点

OAuth 認証を使用した接続に関する、メール配信時の注意点について記載します。

### 自動配信時

タイマーやコマンド等で自動メール配信を行う場合は、次の点に注意して下さい。

OAuth 認証の仕様上、リソースへのアクセス（接続時）のために手動でのサインインや承認操作が発生する場合があります。

この操作は、次の様な場合に発生します。

- アクセストークンとリフレッシュトークンが未取得
- リフレッシュトークンの有効期限切れ
- リフレッシュトークンの取り消し（サインインで使用するアカウント名やパスワード変更時等）

### 対応策

Blue Moon で OAuth 認証の詳細設定を変更した場合や、サインインのアカウント情報を変更した場合は、事前にテスト送信を行っておく。また、Blue Moon を利用する頻度が週1、月1のように少ない場合は、タスクスケジューラー等を利用して1日1回程度の自動テスト送信を行っておくとよいでしょう。

事前にサインインや承認操作を完了させることで、自動配信中のこれらの操作が不要になります。（更新済みのリフレッシュトークンで最新のアクセストークンを自動的に取得できるため）

なお、再度サインインを行う場合に既定の設定では、Blue Moon が確認メッセージダイアログを表示します。Microsoft 365 かつシングルテナントの場合は、このダイアログも自動配信時は非表示にすることを推奨します。非表示にするには、Blue Moon の「環境の設定と管理」で行います。

「メール送信設定」>「認証方式」で OAuth 認証の「詳細設定」>「確認メッセージの表示」